RECEIVED
CENTRAL FAX CENTER
APR 3 0 2007

REMARKS

This paper is responsive to the Office Action dated January 30, 2007. Claims 1-4, 6, 7, 9-17, 27, 29, 30, 35-39, 41, 42, 44-46, 53 and 55 are pending.

Claim Rejection Under 35 U.S.C. § 103

In the Office Action, the Examiner rejected claims 1, 3, 4, 6, 7, 9-11, 13, 14, 27, 30, 35, 37-39, 41-44, 53, and 55 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,473,863 to Genty et al. ("Genty") in view of U.S. Patent Application No. 2002/0083175 to Afek et al. ("Afek"), and further in view of U.S. Patent No. 6,092,113 to Maeshima et al. ("Maeshima"). The Examiner also rejected claims 2 and 36 under 35 U.S.C. 103(a) as being unpatentable over Genty in view of Afek, in view of Maeshima, and further in view of U.S. Patent Application No. 2003/0016679 to Adams et al. (Adams). In addition, the Examiner rejected claims 12, 13, 45, and 46 under 35 U.S.C. 103(a) as being unpatentable over Genty in view of Afek, in view of Maeshima, and further in view of U.S. Patent Application No. 2002/0099854 to Jorgensen. Finally, the Examiner rejected claims 16, 17, and 29 under 35 U.S.C. 103(a) as being unpatentable over Genty in view of Afek, in view of Maeshima, and further in view of U.S. Patent No. 6,880,090 to Shawcross.

Applicant respectfully traverses the rejection. The applied references fail to disclose or suggest the inventions defined by Applicant's claims, and provide no teaching that would have suggested the desirability of modification to arrive at the claimed invention.

Genty, Afek and Maeshima

With respect to the features of independent claims 1, 27, 35 and 53, the Examiner stated that Genty teaches a tunnel between a source and destination, an attack detected, a secondary tunnel established with different addresses, and, upon detecting a network attack, canceling the bandwidth in the packet tunnel. The Examiner also stated that Afek teaches different networks, such as LANs, connected together, and data diverted to guard devices upon detection of an attack by routing data sent to a target device from the source device to the guard devices and then from the guard devices to the target device. The Examiner asserted that Genty and Afek are analogous because they are both related to network protection and that it would have been obvious to a

person of ordinary skill in the art to use the guard devices and redirection taught in Afek with the system in Genty because enhanced protection from distributed denial of service attacks is provided. In addition, the Examiner stated that Maeshima teaches reserving bandwidth for every tunnel on the network. The Examiner asserted that Genty, Afek, and Maeshima are analogous art because they are related to virtual private network setup and that it would have been obvious to a person of ordinary skill in the art to use the bandwidth reservation in Maeshima with the system in Gentry in view of Afek because it is possible to construct a VPN which enables assurance of bandwidth.

Genty, Afek and Maeshima, either singularly or in combination, fail to teach or suggest, in response to the detected network attack, splitting the packet tunnel by selecting an intermediate network device in response to the detected network attack, wherein the intermediate network device has a network address from a network address space other than the address space of the first local area network and the address space of the second local area network, establishing a first packet tunnel from the first local area network to the intermediate network device, and establishing a second packet tunnel that originates from the intermediate network device to the second local area network, as required by Applicant's independent claims 1, 27, 35 and 53.

First, the Genty reference describes establishing a secondary tunnel and abandoning the original tunnel upon detecting a network attack and the Maeshima reference describes reserving bandwidth for every tunnel on a network, the Afek reference merely describes, upon detecting a network attack of a victim device, diverting traffic destined for the victim device from a border router to an associated guard device and then directing the traffic from the associated guard device to the victim device. Thus, Afek fails to describe selecting the guard devices in response to the detected network attack, as required by claim 1. That is, Afek makes no selection of an intermediate network in response to the detected network attack, as required by claim 1. Quite the contrary, according to the Afek reference, paragraph [0257], a pre-defined guard device is placed in each entry next to the border router within the network, and that upon receiving an alert of the detected attack on the victim device, the border routers are set to forward all traffic destined for the victim device to the associated guard device placed next to the border router. Afek merely describes using the guard device associated with the border device in the network to

divert traffic in response to the detected network attack. This is directly contrary to Applicant's claimed invention, which requires selecting an intermediate device in response to the detected network attack. Afek does not disclose responding to a detected network attack on a victim device by selecting a guard device. For at least this reason, Afek does not teach or suggest splitting the packet tunnel by selecting an intermediate network device in response to the detected network attack, wherein the intermediate network device has a network address from a network address space other than the address space of the first local area network and the address space of the second local area network, establishing a first packet tunnel from the first local area network to the intermediate network device, and establishing a second packet tunnel that originates from the intermediate network device to the second local area network, as required by Applicant's independent claims, as required by Applicant's independent claims 1, 27, 35 and 53.

Second, directly counter to Applicant's claims, Afek does not disclose the guard device having a network address from a network address space *other than the address space of the first local area network and the address space of the second local area network.* Afek describes using the guard device positioned next to the border router to divert traffic destined for the victim device upon detecting the network attack. Afek makes no suggestion of the guard device having a network address from a different network address space than the address space of the border router and the address space of the victim router. In fact, Afek only discusses network addresses of devices in the network in relation to the victim device having both a public network address and a private network address used by the guard devices upon the network attack, paragraph [0255]. In paragraph [0265], Afek discloses that the private network address of the victim device may be from a private network address space different than the address space of the public network address. Thus, contrary to Applicant's claims, Afek fails to describe splitting the packet tunnel by selecting an intermediate network device in response to the detected network attack, wherein the intermediate network device has a network address from a network address space other than the address space of the first local area network and the address space of the second local area network, as required by Applicant's independent claims 1, 27, 35 and 53.

To be clear, Genty in view of Afek and Maeshima suffers from the exact problem described and solved by the Applicant's claimed technique, i.e., the problem of limited address space diversity. Any diverted traffic in Afek would be sourced at the border router and

terminated at the associated guard device within the ***same address spaces*** as the original source and destination devices and, therefore, would continue to be highly susceptible to address spoofing. Applicant's claimed technique directly overcomes this problem.

Third, the cited referenced fail to achieve the structural arrangement of tunnels recited in the claims. Afek does not describe establishing a first packet tunnel from the first local area network to the intermediate network device, and establishing a second packet tunnel that originates from the intermediate network device to the second local area network, as required by Applicant's independent claims. Afek fails to mention establishing network tunnels at any time and certainly does not teach establishing network tunnels in response to the detected network attack. According to the Afek reference, paragraph [0252], upon detecting a network attack, the victim device alerts the guard devices through communication channels supplied by the backbone provider of the network. Paragraph [0250] of the Afek references discloses that the border routers associated with the guard devices then divert traffic destined for the victim device to the associated guard devices, causing that traffic to take a path that it would not normally take if there was no network attack. Afek merely describes communicating between network devices and diverting packets to guard devices via communication channels on the existing backbone of the network. However, Afek fails to mention establishing network tunnels between the border routers and the associated guard devices, and establishing network tunnels between the guard devices and the victim device. Thus, even if the teachings of Genty were modified by the teachings of Afek and Maeshima as suggested by the Examiner, the combined references would not result in Applicant's invention as claimed. For example, Genty in view of Maeshima would suggest establishing a secondary tunnel and entirely abandoning the original tunnel upon detecting a network attack, and reserving bandwidth for the new tunnel. Afek describes diverting traffic destined for a victim device from a border router to an associated guard device along an established communication channel upon detecting a network attack of the victim device. Combining the references would result in a system that, upon detecting a network attack, abandoning the tunnel between the border router and the victim device, establishing a new tunnel in its place between the border router and the victim, diverting traffic from the border router to the associated guard device using the new tunnel (which would effectively bypass the new tunnel). The combined teachings fails to result in a system that splits a network tunnel between a

first and second local area network by utilizing an intermediate device selected to have a network address from a network address space other than the address space of the first local area network and the address space of the second local area network. There is no suggestion of establishing two new network tunnels, i.e., a network tunnel between the source device and the intermediate device and a network tunnel between the selected intermediate device and the destination device, as required by Applicant's independent claims 1, 27, 35, and 53. There is no suggestion for this approach in any of the references, even when combined. Quite the contrary, the system proposed by the Examiner would still require that the traffic flow through the Border router and then diverted to the Guard device. Thus, there simply would not be tunnels established between

Additionally, many of Applicant's dependent claims are directed to techniques by which the source device and the destination device cooperate so as to select an intermediate device and split the tunnel in response to a network attack in the manner recited in the independent claim 1. Claim 6, for example, recites exchanging a set of available network addresses between the source network device and the destination network device, wherein the set of available network addresses correspond to a plurality of intermediate network devices. Claim 7 requires maintaining a set of available network addresses for a plurality of available intermediate network devices, wherein the network addresses are within network address spaces other than the address space of the first local area network and the address space of the second local area network, and selecting one of the network addresses. None of the references, either singularly or in combination, teach or suggest these elements.

For at least these reasons, Applicant's independent claims 1, 27, 35 and 53 are in condition for allowance, as are Applicant's dependent claims 3, 4, 6, 7, 9-17, 29, 30, 36-39, 41, 42, 44-46 and 55.

Genty, Afek, Maeshima and Adams

As described above, Genty, Afek and Maeshima do not teach or suggest, in response to the detected network attack, splitting the packet tunnel by selecting an intermediate network device, wherein the intermediate network device has a network address from a network address space other than the address space of the first local area network and the address space of the second local area network, establishing a first packet tunnel from the first local area network to

the intermediate network device, and establishing a second packet tunnel that originates from the intermediate network device to the second local area network, as recited by Applicant's independent claims 1 and 35 from which claims 2 and 36 depend. Adams fails to provide any teaching capable of overcoming the deficiencies of Genty, Afek and Maeshima.

Genty, Afek, Maeshima and Jorgensen

As described above, Genty, Afek and Maeshima do not teach or suggest, in response to the detected network attack, splitting the packet tunnel by selecting an intermediate network device, wherein the intermediate network device has a network address from a network address space other than the address space of the first local area network and the address space of the second local area network, establishing a first packet tunnel from the first local area network to the intermediate network device, and establishing a second packet tunnel that originates from the intermediate network device to the second local area network, as recited by Applicant's independent claims 1 and 35 from which claims 12, 13, 45 and 46 depend. Jorgensen fails to provide any teaching capable of overcoming the deficiencies of Genty, Afek and Maeshima.

Genty, Afek, Maeshima and Shawcross

As described above, Genty, Afek and Maeshima do not teach or suggest, in response to the detected network attack, splitting the packet tunnel by selecting an intermediate network device, wherein the intermediate network device has a network address from a network address space other than the address space of the first local area network and the address space of the second local area network, establishing a first packet tunnel from the first local area network to the intermediate network device, and establishing a second packet tunnel that originates from the intermediate network device to the second local area network, as recited by Applicant's independent claims 1 and 27 from which claims 16, 17 and 29 depend. Shawcross fails to provide any teaching capable of overcoming the deficiencies of Genty, Afek and Maeshima.

For at least these reasons, the Examiner has failed to establish a prima facie case for non-patentability of Applicant's claims 1-4, 6, 7, 9-17, 27, 29, 30, 35-39, 41, 42, 44-46, 53 and 55 under 35 U.S.C. 103(a). Withdrawal of this rejection is requested.

RECEIVED
CENTRAL FAX CENTER

APR 3 0 2007

CONCLUSION

All claims in this application are in condition for allowance. Applicant respectfully requests reconsideration and prompt allowance of all pending claims. Please charge any additional fees or credit any overpayment to deposit account number 50-1778. The Examiner is invited to telephone the below-signed attorney to discuss this application.

Date: April 30, 2007

By: Kent J. Sieffert

SHUMAKER & SIEFFERT, P.A.
1625 Radio Drive, Suite 300
Woodbury, Minnesota 55125
Telephone: 651.735.1100
Facsimile: 651.735.1102

Name: Kent J. Sieffert
Reg. No.: 41,312